AI+ Security Compliance™

AI CERTs

Com certificação

- **Nível:**
- **Duração:** 40h

Sobre o curso

A certificação **AI+ Security Compliance™** foi desenvolvida para capacitar profissionais a integrar a Inteligência Artificial em práticas de cibersegurança, compliance e governação, de forma estruturada, prática e alinhada com os requisitos regulatórios atuais. O foco está na utilização da IA para garantir conformidade, mitigar riscos e reforçar a segurança em ambientes digitais complexos e altamente regulados.

Ao longo do percurso, os participantes exploram como aplicar IA em frameworks de compliance, gestão de risco e auditoria, incluindo alinhamento com normas internacionais como ISO, NIST e GDPR. São abordados temas como proteção de dados, arquitetura segura, controlo de acessos e monitorização contínua com IA, permitindo uma visão integrada da segurança e conformidade em sistemas modernos.

A componente prática assume um papel relevante, com estudos de caso e aplicação de ferramentas que permitem implementar estratégias de compliance automatizado, realizar avaliações de risco e garantir a conformidade contínua em ambientes organizacionais

Em parceria com a Rumos, Platinum Gold Partner.

Destinatários

- Profissionais de cibersegurança e segurança da informação;
- Especialistas em compliance, risco e auditoria;
- Analistas e gestores de IT responsáveis por segurança e governação;
- Consultores e profissionais envolvidos em regulamentação e proteção de dados;
- Líderes tecnológicos que pretendam assegurar conformidade em sistemas baseados em IA.

Objetivos

- Compreender a integração entre Inteligência Artificial, cibersegurança e compliance;
- Aplicar IA na gestão de risco e avaliação contínua de conformidade;
- Implementar estratégias de proteção de dados e privacidade com IA;
- Desenvolver arquiteturas seguras e alinhadas com normas regulatórias;
- Automatizar processos de auditoria e monitorização de segurança;
- Integrar IA em práticas de IAM e resposta a incidentes;
- Garantir governação, ética e conformidade em sistemas baseados em IA.

Condições

Detalhes do exame

- Duração: 90 minutos;
- Pontuação mínima de aprovação: 70% (35/50);
- Formato: 50 questões de escolha múltipla e múltipla resposta;
- Realização online, através de plataforma com proctoring por IA e agendamento flexível.

Pré-requisitos

- Conhecimentos básicos de cibersegurança e compliance;
- Familiaridade com conceitos de gestão de risco e proteção de dados;
- Interesse em aplicar IA em contextos de segurança e regulamentação;
- Experiência em ambientes IT é recomendada, mas não obrigatória

Metodologia

A formação decorre em formato e-learning, com aproximadamente 40 horas de conteúdos on-demand, incluindo vídeos, e-book, podcasts e atividades práticas interativas. A aprendizagem pode ser realizada em qualquer momento e a partir de qualquer lugar, com quizzes modulares para acompanhar o progresso.

Programa

- Course Introduction
- Introduction to Cybersecurity Compliance and AI
- Security and Risk Management with AI
- Asset Security and Privacy Compliance with AI
- Security Architecture and Engineering with AI

- Network and Communication Security with AI
- Identity and Access Management (IAM) and Incident Response with AI
- Security Operations, Software Security, and Audit with AI
- Future Trends and Governance in AI Security Compliance

Course Introduction

Introduction to Cybersecurity Compliance and AI

- Overview of cybersecurity compliance principles
- Key international compliance standards (ISO, NIST, GDPR, etc.)
- Building and implementing compliance programs
- Role of AI in strengthening cybersecurity compliance
- Real-world compliance case studies

Security and Risk Management with AI

- Risk management frameworks and methodologies
- Conducting risk assessments and gap analysis
- Using AI for continuous risk assessment
- Incident response planning supported by AI
- Aligning compliance with risk governance

Asset Security and Privacy Compliance with AI

- Data classification and information protection
- AI-driven privacy protection techniques
- Asset management and monitoring using AI
- Regulatory requirements for data protection
- Best practices and compliance case studies

Security Architecture and Engineering with AI

- Secure design principles and compliance-by-design
- AI applications in cryptography
- AI-assisted vulnerability assessment
- Security models and architecture frameworks
- Engineering compliant and resilient systems

Network and Communication Security with AI

- Network security fundamentals and compliance controls
- AI-driven network monitoring and defense
- Detecting threats and anomalies using AI
- Compliance requirements for network security
- AI-enabled network defense strategies

Identity and Access Management (IAM) and Incident Response with AI

- IAM fundamentals and compliance requirements
- AI-based identity verification and access control
- Managing IAM threats using AI
- AI-driven security testing and incident response
- Continuous monitoring and legal considerations

Security Operations, Software Security, and Audit with AI

- AI-powered Security Operations Center (SOC)
- Privacy compliance and disaster recovery
- Secure Software Development Life Cycle (SDLC)
- AI in application security testing and DevSecOps
- Internal and external audits with AI support

Future Trends and Governance in AI Security Compliance

- Emerging AI technologies in cybersecurity
- AI in cyber threat intelligence
- Quantum computing implications
- Ethical AI, governance, and regulatory evolution
- Practical applications and future-ready compliance strategies